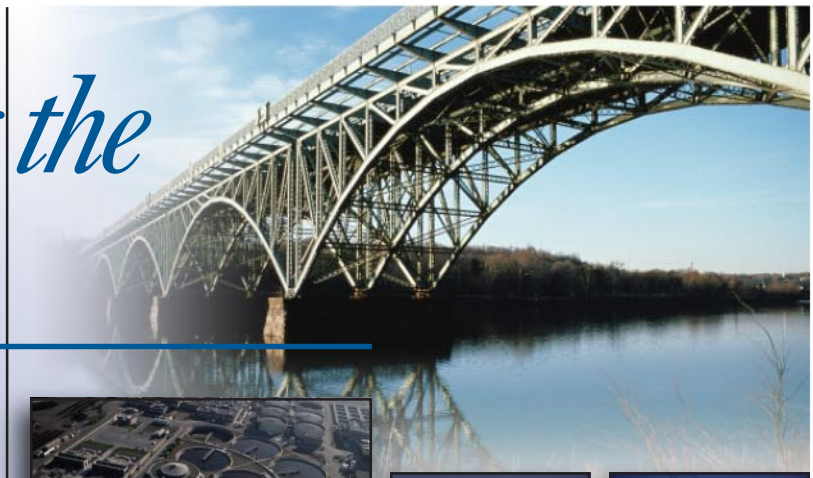
Strengthening the Nation's Core



National Security

Control Systems Security & Test Center

A Department of Homeland Security program to secure national infrastructure

Threats to Control Systems

Many of the nation's critical infrastructures, such as refineries, transportation systems and telecommunications rely on sophisticated computer-based control systems to monitor and operate daily tasks. These automated systems collect data from the field, process and display this information for operators and send control commands to local and remote equipment.

As identified by the Government Accountability Office, these control systems, though efficient, are vulnerable to cyber attacks by hackers, virus writers, foreign intelligence services and various other criminal organizations.

Without proper security, intruders can potentially gain access to these critical infrastructure control systems compromising, disabling and disrupting their essential functions. These actions could endanger public safety and economic stability.

DHS Response

The Department of Homeland Security (DHS) has develop a strategy to swiftly identify and prioritize infrastructure vulnerabilities, address them directly where possible and provide the technology and training to ensure effective solutions.

Crucial to this strategy is the support that the Idaho National Laboratory's Control Systems Security and Test Center provides to DHS and the U.S. Computer Emergency Readiness Team (CERT). This facility is designed to test equipment and procedures for inherent vulnerabilities while providing awareness and tool development to the control system community.

Continued on back

INL
Idaho National Laboratory

Continued from front

The CSSTC creates a centralized location for industry, vendors and government agencies to work together to reduce cyber vulnerabilities in control systems. The facility and expert staff are capable of running mock exercises and calculated scenarios on full-scale control systems in a state-of-the-art research and testing facility. Results are compiled and potential improvements are noted and sent to the equipment vendors for consideration.

Program Objectives

The CSSTC performs work in multiple objective areas. These include industry outreach and awareness, control system vulnerability assessments, risk assessments, analysis and tool development, and supporting US-CERT emergency response.

Securing the Future

The CSSTC employs control system experts to gather field data, analyze existing systems and identify specific threats and vulnerabilities. The objective is to expedite the development of next generation, cyber secure control systems by providing customers with relevant data, research facilities and highly trained, technical staff.

The CSSTC has the ability to perform vulnerability assessments on all types of control systems and associated components in a real-life operating infrastructure environment.

Technical solutions in the private sector will be leveraged to eliminate vulnerabilities. At the same time, the CSSTC works with closely with key national resources including other federal laboratories, industry experts, trade groups, academia and federal, state and local governments.

Vulnerability assessments enable the CSSTC to formulate an integrated national response to:

- Identify and reduce control system vulnerabilities
- Help industry identify sector needs and security objectives
- Share sanitized information to facilitate improved designs
- Foster an environment for increasing awareness of control system cyber security

Awareness and Response

Plans are currently being developed to provide continuous support to the control systems division of the US-CERT. This role would allow control systems experts from the CSSTC to responds to emerging control system cyber security issues and works with the US-CERT to provide analysis and solutions.

Industry Tools

Along with testing, evaluating and performing analysis on control systems, the CSSTC is developing security assurance levels for the control system industry and equipment vendors. Assurance levels provide a basis for improved security requirements based on the importance of each critical infrastructure and its potential for cascading effects on human health, environment, economy and national security.

The CSSTC is also creating a secure database to share information, research, and potential threats with the industry. The database will be validated and secure to protect specific stakeholder and national interests, and will provide information that has been sensitized of proprietary information.

The use of this database is scheduled to start in mid-2005.

Program Objectives

Funded by the Department of Homeland Security, the CSSTC is dedicated to providing support and solutions to the control systems division of the US-CERT. Employees of the CSSTC represent a broad spectrum of talents and expertise in industry sectors including the oil and gas sector, chemical industry, electric utilities, cyber security and many others. Our mission is to provide real solutions to the industry and vendors to help reduce and eliminate vulnerabilities in the control systems that operate our nation's critical infrastructures.

For more information:

Julio Rodriquez, INL
(208) 526-2039
Julio.Rodriguez@inl.gov

http://csstc.inel.gov

A U.S. Department of Energy National Laboratory

The CSSTC is located at the INEEL's Information Operation Research Center (IORC).